6

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/626,054	07/23/2003	Martin S. Casden	DE038	1432

7590 03/21/2007

Natan Epstein, Esq.
Law Offices of Natan Epstein
9th Floor
11377 West Olympic Boulevard
Los Angeles, CA 90064

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	PAPER NUMBER
2134	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/21/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	**Application No.** 10/626,054	**Applicant(s)** CASDEN ET AL.	
	Examiner Michael J. Simitoski	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 July 2003*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *23 July 2003* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *7/5/2005*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. The IDS of 7/5/2005 was received and considered.

2. Claims 1-16 are pending.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-6, 8-13 & 15-16 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent 5,310,999 to Claus et al. (**Claus**).

Regarding claim 1, Claus discloses a method of encrypting identification tags of the type having a data storage for storing a fixed tag UID (Card ID, col. 9, lines 34-39) unique to each of said tags and variable user data (variable data frame, col. 9, lines 61-65), said tag UID and said user data being readable by a tag reader, said method comprising the steps of: providing an identification tag (transponder) having a permanent UID stored thereon (Card ID, col. 9, lines 34-39 & col. 10, lines 18-20), providing an encryption engine operative for encrypting user data with an encryption key (variable data frame is encrypted, col. 9, line 61 – col. 10, line 12), entering said UID to provide part or all of said encryption key (col. 9, lines 34-39), entering user data (variable data frame) for encryption by said engine (col. 9, line 61 – col. 10, line 12), encrypting said user data with said encryption key (secret code) to derive encrypted user data (col. 10, lines 10-12 & Fig. 14) and storing said encrypted user data (variable data frame in said data storage of said identification tag (col. 9, lines 63-65).

Regarding claim 2, Claus discloses wherein said tag is an RFID tag (transponder, col. 9, lines 24-25) and said data storage is readable by an RFID reader (antenna/Plaza, col. 9, lines 21-25 & Fig. 3, #320).

Regarding claim 3, Claus discloses wherein said encryption engine (Plaza reader) comprises an encryption algorithm running on a digital processor platform (Plaza) enabled for reading an writing to said data storage (col. 9, line 61 – col. 10, line 12).

Regarding claim 4, Claus discloses wherein said digital processor platform is operatively associated with an RFID reader for reading and writing to said data storage (col. 9, lines 24-25 & Fig. 3, #320).

Regarding claim 5, Claus discloses wherein said encryption algorithm is a DES encryption algorithm (col. 9, lines 51-52).

Regarding claim 6, Claus discloses wherein said encryption key (secret code) is a final key based on a combination of said tag UID (Card ID) and a private key (secret algorithm, col. 9, lines 36-39).

Regarding claim 8, Claus discloses providing a decryption engine (Plaza/reader, Fig. 3, #320) operative for decrypting said encrypted user data (variable data frame) with an encryption key (secret code, col. 9, lines 40-60), presenting an encrypted identification tag for reading (col. 9, lines 40-60), reading said tag UID (Card ID) and said encrypted user data stored on said encrypted identification tag (variable data frame, col. 9, lines 40-56), providing said tag UID to said decryption engine (Plaza/reader) for deriving said encryption key (secret code, col. 9, lines

36-39), providing said encrypted user data (variable data frame) to said decryption engine (Plaza/reader) for decryption with said decryption key (secret code, col. 9, lines 52-60) and decrypting said encrypted user data with said decryption engine to derive decrypted user data (variable data frame, col. 9, lines 35-60).

Regarding claim 9, Claus discloses wherein said encrypted identification tag is an RFID tag (transponder, col. 9, lines 24-25) and said tag is readable by an RFID reader (antenna/Plaza, col. 9, lines 21-25 & Fig. 3, #320).

Regarding claim 10, Claus discloses wherein said decryption engine (Plaza/reader) comprises a decryption algorithm running on a digital processor platform enabled for reading an writing to said encrypted identification tag (col. 9, lines 61-65).

Regarding claim 11, Claus discloses wherein said digital processor platform (Plaza/reader) is operatively associated with an RFID reader for reading and writing to said encrypted identification tag (col. 9, line 61 – col. 10, line 12).

Regarding claim 12, Claus discloses wherein said decryption algorithm is a DES decryption algorithm (col. 9, lines 51-52).

Regarding claim 13, Claus discloses wherein said encryption key (secret code) is a final key based on a combination of said tag UID (Card ID) and a private key (secret algorithm, col. 9, lines 36-39).

Regarding claim 15, Claus discloses generating a key (secret code) based in part or in whole on said UID (Card ID, col. 9, lines 36-39) code of one said tag (transponder), encrypting said user data with said key to derive encrypted user data (variable data frame, col. 9, line 61 – col. 10, line 12) for storage on said one tag (col. 9, lines 61-65), and decrypted encrypted user data read from said one tag with said key (secret code, col. 9, line 40-60), such that a unique key (secret code) is generated for encryption and decryption of user data on each tag (col. 9, lines 36-39).

Regarding claim 16, Claus discloses wherein said identification tags (transponders) are RFID tags (col. 9, lines 24-25, col. 9, lines 21-25 & Fig. 3, #320).

5. Claims 1, 3, 6, 8, 10, 13 & 15 are rejected under 35 U.S.C. 102(b) as being anticipated by European Patent Application EP 1 050 887 to Hirota et al. (**Hirota**).

Regarding claim 1, Hirota discloses a method of encrypting identification tags (memory card, ¶84) having a data storage (ROM, ¶67) for storing a fixed tag UID (medium ID, ¶84) unique to each of said tags (¶67) and variable user data (content, ¶84), said tag UID (medium ID) and said user data (content) being readable by a tag reader (PC, ¶84 & ¶99), said method comprising the steps of providing an identification tag (memory card, ¶84) having a permanent UID stored thereon (medium ID, ¶67), providing an encryption engine (CPU, Fig. 4 & ¶98(5)), operative for encrypting user data (content) with an encryption key (password, ¶98(5)), entering said UID (medium ID) to provide part or all of said encryption key (¶98(2)), entering user data (content) for encryption by said engine, encrypting said user data with said encryption key (password) to derive encrypted user data (¶98(5)) and storing said encrypted user data in said data storage of said identification tag (¶98(5)).

Regarding claim 3, Hirota discloses wherein said encryption engine (PC) comprises an encryption algorithm running on a digital processor platform enabled for reading and writing to said data storage (¶98(5)).

Regarding claim 6, Hirota discloses wherein said encryption key (password) is a final key based on a combination of said tag UID (medium ID) and a private key (master key, ¶98(3)).

Regarding claim 8, Hirota discloses providing a decryption engine (PC, Fig. 4) operative for decrypting said encrypted user data with (¶99(4-5)) an encryption key (password, ¶99(5)), presenting an encrypted identification tag (memory card) for reading (¶99(2)), reading said tag UID (medium ID, ¶99(2)) and said encrypted user data (content, ¶99(5)) stored on said encrypted identification tag (memory card), providing said tag UID (medium ID) to said decryption engine for deriving said encryption key (extracting the password, ¶99(4)), providing said encrypted user data (encrypted content) to said decryption engine for decryption with said encryption key (password, ¶99(5)) and decrypting said encrypted user data with said decryption engine to derive decrypted user data (¶99(5)).

Regarding claim 10, Hirota discloses wherein said encryption engine (PC) comprises an encryption algorithm running on a digital processor platform enabled for reading and writing to said data storage (¶98(5)).

Regarding claim 13, Hirota discloses wherein said encryption key (password) is a final key based on a combination of said tag UID (medium ID) and a private key (master key, ¶98(3)).

Regarding claim 15, Hirota discloses generating a key (password) based in part or in whole on said UID code of one said tag (medium ID of memory card, ¶98(2-3)), encrypting said user data (content) with said key (password) to derive encrypted user data for storage on said one tag (¶98(5)), and decrypting encrypted user data (content) read from said one tag with said key (password, ¶99(5)), such that a unique key is generated for encryption and decryption of user data on each tag (¶67 & ¶98(2-3)).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 7 & 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Hirota**, as applied to claims 6 & 13, in view of U.S. Patent Application Publication 2005/0004875 to Kontio et al. (**Kontio**).

Regarding claims 7 & 14, Hirota lacks wherein the final key is derived by XORing said private key with said tag UID. However, Kontio teaches that in encrypting media content, it is known to derive the encryption key (final key) by XORing a media ID (unique to the media) with a key token (¶58), which protects the key. This is useful in joining the media with the specific tangible medium. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Hirota to derive the password by XORing the medium ID with the master key. One of ordinary skill in the art would have been motivated to perform such a modification to protect the password in a known manner and to join the content with the memory card.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MJS

March 15, 2007

KAMBIZ ZAND
PRIMARY EXAMINER